Previous Doc Next Doc Go to Doc#
First Hit

Generate Collection

L1: Entry 7 of 7 File: JPAB Oct 26, 2001

PUB-NO: JP02001298779A
DOCUMENT-IDENTIFIER: JP 2001298779 A
TITLE: MOBILE INFORMATION TERMINAL AND SERVICE SYSTEM USING IT

PUBN-DATE: October 26, 2001

INVENTOR-INFORMATION:
NAME COUNTRY
TAKAHASHI, KIYOSHI

ASSIGNEE-INFORMATION:
NAME COUNTRY
MITSUBISHI ELECTRIC CORP

APPL-NO: JP2000113594
APPL-DATE: April 14, 2000

INT-CL (IPC): H04Q 7/38; G09C 1/00; H04L 9/32; H04M 1/67; H04M 3/00; H04M 3/42; H04M 11/00

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a mobile information terminal that can receive services after authentication of a user once and to provide a service system using it.

SOLUTION: The service system is provided with a data processing unit that collates fingerprint data and a terminal identification code sent from the mobile information terminal with fingerprint data-terminal identification code information that cross-references fingerprint data of a person registered as a user of the mobile information terminal and a terminal identification code identifying the mobile information terminal and issues an authentication code with a validity on the basis of the result of collation, the mobile information terminal that reads the fingerprint, generates the fingerprint data, transmits the fingerprint data and the terminal identification code stored in advance to the data processing print and stores the received authentication code and the validity, and a service terminal that receives the authentication code. The service system provides services to the user of the mobile information terminal on the basis of the authentication code received by the service terminal.



Previous Doc Next Doc Go to Doc#

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－298779
（P2001－298779A）
(43)公開日　平成13年10月26日(2001.10.26)

| (51)Int.Cl.' | | 識別記号 | Ｆ Ｉ | | テーマコード'(参考) | |
|---|---|---|---|---|---|---|
| Ｈ０４Ｑ | 7/38 | | Ｇ０９Ｃ | 1/00 | ６６０Ｅ | ５Ｊ１０４ |
| Ｇ０９Ｃ | 1/00 | ６６０ | Ｈ０４Ｍ | 1/67 | | ５Ｋ０２４ |
| Ｈ０４Ｌ | 9/32 | | | 3/00 | Ｂ | ５Ｋ０２７ |
| Ｈ０４Ｍ | 1/67 | | | 3/42 | Ｚ | ５Ｋ０５１ |
| | 3/00 | | | 11/00 | ３０２ | ５Ｋ０６７ |

審査請求　未請求　請求項の数12　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2000－113594(P2000－113594)

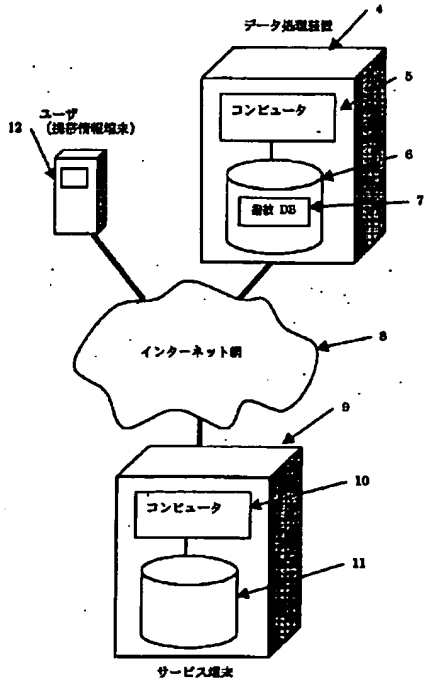
(22)出願日　平成12年４月14日(2000.4.14)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　高橋　清
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100102439
弁理士　宮田　金雄　（外１名）

最終頁に続く

(54)【発明の名称】　携帯情報端末およびこれを用いたサービスシステム

(57)【要約】
【課題】　一度の本人認証を行うことにより、複数のサービスの提供を受けることができる携帯情報端末とこれを用いたサービスシステムを提供する。
【解決手段】　携帯情報端末の使用者として登録された者の指紋データと携帯情報端末を識別する端末識別符号とを対応させた指紋データー端末識別符号情報に、携帯情報端末から送信された指紋データと端末識別符号を照合し、この照合結果に基づき有効期限を付けた認証符号を発行するデータ処理装置と、指紋を読み取り指紋データを生成し、指紋データとあらかじめ記憶された端末識別符号をデータ処理装置へ送信し、受信した認証符号と有効期限を記憶する携帯情報端末と、認証符号を受信するサービス端末とを含み、サービス端末で受信された認証符号に基づいて携帯情報端末の使用者へサービスが提供されるサービスシステム。



1

【特許請求の範囲】

【請求項1】　携帯情報端末の使用者として登録された者の指紋データと前記携帯情報端末を識別する端末識別符号とを対応させた指紋データ－端末識別符号情報に、前記携帯情報端末から送信された指紋データと端末識別符号を照合し、この照合結果に基づき有効期限を付けた認証符号を発行するデータ処理装置と通信を行うものであって、指紋を読み取り指紋データを生成する指紋読み取り手段、前記指紋データと、あらかじめ記憶された前記端末識別符号とを前記データ処理装置へ送信する送信部、前記データ処理装置において発行された認証符号を受信する受信部、およびこの受信部で受信された前記認証符号と有効期限をあわせて記憶する記憶部を備えたことを特徴とする携帯情報端末。

【請求項2】　送信する前記指紋データを暗号化する暗号化手段、および暗号化され受信された前記認証符号を復号化する復号化手段を備えたことを特徴とする請求項1に記載の携帯情報端末。

【請求項3】　前記暗号化には、公開鍵暗号方式を用いることを特徴とする請求項2に記載の携帯情報端末。

【請求項4】　送信する前記指紋データ、および受信する前記認証符号が圧縮コード化されていることを特徴とする請求項1に記載の携帯情報端末。

【請求項5】　前記データ処理装置より受信した認証符号とその有効期限をあわせて表示する表示手段を備えたことを特徴とする請求項1に記載の携帯情報端末。

【請求項6】　前記記憶部に記憶した認証符号を、無効にする手段を備えたことを特徴とする請求項1に記載の携帯情報端末。

【請求項7】　通信機能の操作を行う通信機能操作部を備え、この通信機能操作部の何れかのキー操作に応じて指紋を読み取る手段を設けたことを特徴とする請求項1に記載の携帯情報端末。

【請求項8】　前記通信機能操作部のうち、データ通信開始キーの操作に応じて指紋を読み取る手段を設けたことを特徴とする請求項7に記載の携帯情報端末。

【請求項9】　前記通信機能操作部のうち、通話開始キーの操作に応じて指紋を読み取る手段を設けたことを特徴とする請求項7に記載の携帯情報端末。

【請求項10】　使用者の指紋データをあらかじめ記憶させた第2の記憶部、前記指紋読み取り手段において読み取られた指紋データと前記あらかじめ記憶された指紋データとを照合する照合手段を備え、この照合結果に基づいて、前記指紋データと前記端末識別符号を前記データ処理装置へ送信することを特徴とする請求項1に記載の携帯情報端末。

【請求項11】　携帯情報端末の使用者として登録された者の指紋データと前記携帯情報端末を識別する端末識別符号とを対応させた指紋データ－端末識別符号情報を記憶する記憶部と、この指紋データ－端末識別符号情報

2

に、前記携帯情報端末から送信された指紋データと端末識別符号を照合する照合手段とを備え、この照合結果に基づいて有効期限を付けた認証符号を発行するデータ処理装置、指紋を読み取る指紋読み取り手段と、この指紋読み取り手段において読み取られた指紋データとあらかじめ記憶された前記端末識別符号とを前記データ処理装置へ送信する送信部と、前記データ処理装置が発行した認証符号を受信する受信部と、前記認証符号と有効期限をあわせて記憶する記憶部とを備えた携帯情報端末、および前記認証符号を受信するサービス端末を含み、サービス端末で受信された認証符号に基づいて携帯情報端末の使用者へ希望するサービスが提供されるサービスシステム。

【請求項12】　前記携帯情報端末と前記データ処理装置との通信の中継を行う交換機を含み、この交換機は、認証符号およびサービス提供依頼が前記サービス端末へ送信される際に、認証符号をあらかじめ定められた対応する音声信号に変換し、この音声信号を前記サービス端末へ送信することを特徴とする請求項11に記載のサービスシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、指紋読み取り手段を備えた携帯情報端末とこれを用いたサービスシステムに関するものである。

【0002】

【従来の技術】例えば、指紋データを用いた本人認証およびサービス提供システムとしては、特開平11－96252号に記載されたものがある。この従来システムは、まずユーザが携帯端末より商品購入指示を出すと、携帯端末で採取した網膜パターンデータおよび指紋データを、あらかじめ口座開設時に網膜パターンデータと指紋データを登録してある銀行へ送信する。次に銀行は送信されたデータと登録してあるデータの照合により本人認証を行い、本人認証にパスすれば、ユーザに対して口座の残高情報を返信する。さらに残高情報を受信したユーザと、このユーザが取引を行った相手は、それぞれ取引結果を前記本人認証を行った銀行へ送信し、これにより銀行において決済が行われるというものである。

【0003】

【発明が解決しようとする課題】以上のような従来のシステムにおいては、商取引を行う度に決済を行う銀行で本人認証を行う必要があり、商取引時のユーザおよび銀行の作業が煩雑になるという問題点があった。また、ユーザはあらかじめ網膜パターンデータおよび指紋データの登録を、決済に利用するすべての銀行に対し行わなければならない、もしくはあらかじめ登録を行った銀行を利用しなければサービスを受けられず、使い勝手が悪いという問題点があった。

【0004】この発明は上記のような問題点を解決する

ためなされたもので、第1の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができる携帯情報端末を提供することである。

【0005】また、第2の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、セキュリティに優れた携帯情報端末を提供することである。

【0006】また、第3の目的は、インターネットを利用して、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、セキュリティに優れた携帯情報端末を提供することである。

【0007】また、第4の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、送受信するデータ量の少ない携帯情報端末を提供することである。

【0008】また、第5の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、使い勝手の良い携帯情報端末を提供することである。

【0009】また、第6の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、本人以外が不正にサービスの提供を受けることを防止できる携帯情報端末を提供することである。

【0010】また、第7の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、利用者の制限が可能な携帯情報端末を提供することである。

【0011】また、第8の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるサービスシステムを提供することである。

【0012】また、第9の目的は、一度の本人認証を行うことにより、複数のサービスの提供を受けることができるとともに、サービス端末の使い勝手が良いサービスシステムを提供することである。

【0013】

【課題を解決するための手段】この発明に係る携帯情報端末は、携帯情報端末の使用者として登録された者の指紋データと携帯情報端末を識別する端末識別符号とを対応させた指紋データ－端末識別符号情報に、携帯情報端末から送信された指紋データと端末識別符号を照合し、この照合結果に基づき有効期限を付けた認証符号を発行するデータ処理装置と通信を行うものであって、指紋を読み取り指紋データを生成する指紋読み取り手段、指紋データとあらかじめ記憶された端末識別符号をデータ処理装置へ送信する送信部、認証符号を受信する受信部、および受信した認証符号と有効期限を記憶する記憶部を備えるようにしたものである。

【0014】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、送信する指紋データを暗号化する暗号化手段、および暗号化され受信された認証符号を復号化する復号化手段を備えるようにしたものである。

【0015】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、送信する指紋データを暗号化する暗号化手段、および暗号化され受信された認証符号を復号化する復号化手段を備え、暗号化には公開鍵暗号方式を用いるようにしたものである。

【0016】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部を備え、送信する指紋データおよび受信する認証符号を圧縮コード化するようにしたものである。

【0017】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、受信した認証符号とその有効期限を表示する表示手段を備えるようにしたものである。

【0018】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前期記憶部に加え、記憶部に記憶した認証符号を、無効にする手段を備えるようにしたものである。

【0019】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、通信機能の操作を行う通信機能操作部を備え、通信機能操作部の何れかのキー操作に応じて指紋を読み取る手段を設けるようにしたものである。

【0020】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、通信機能の操作を行う通信機能操作部を備え、通信機能操作部のうち、データ通信開始キーの操作に応じて指紋を読み取る手段を設けるようにしたものである。

【0021】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、通信機能の操作を行う通信機能操作部を備え、通信機能操作部のうち、通話開始キーの操作に応じて指紋を読み取る手段を設けるようにしたものである。

【0022】また、この発明に係る携帯情報端末は、前記指紋読み取り手段、前記送信部、前記受信部、前記記憶部に加え、使用者の指紋データをあらかじめ記憶している第2の記憶部、および読み取られた指紋データと記憶している指紋データとを照合する照合手段を備え、照合結果に基づいて、指紋データと端末識別符号をデータ処理装置へ送信するようにしたものである。

【0023】また、この発明に係るサービスシステムは、携帯情報端末の使用者として登録された者の指紋データと携帯情報端末を識別する端末識別符号とを対応させた指紋データ－端末識別符号情報を記憶する記憶部と、指紋データ－端末識別符号情報に、携帯情報端末から送信された指紋データと端末識別符号を照合する照合

手段とを備え、照合結果に基づいて有効期限を付けた認証符号を発行するデータ処理装置、指紋を読み取る指紋読み取り手段と、読み取られた指紋データとあらかじめ記憶された端末識別符号をデータ処理装置へ送信する送信部と、認証符号を受信する受信部と、受信した認証符号と有効期限を記憶する記憶部とを備えた携帯情報端末、および認証符号を受信するサービス端末を含み、サービス端末で受信された認証符号に基づいて携帯情報端末の使用者へ希望するサービスが提供されるようにしたものである。

【００２４】また、この発明に係るサービスシステムは、前記データ処理装置と、前記携帯情報端末と、前記サービス端末に加え、携帯情報端末とデータ処理装置との通信の中継を行う交換機を含み、交換機が認証符号およびサービス提供依頼がサービス端末へ送信される際に、認証符号をあらかじめ定められた対応する音声信号に変換し、この音声信号をサービス端末へ送信するようにしたものである。

【００２５】

【発明の実施の形態】実施の形態１．図１は、この発明の実施の形態１における携帯情報端末の外観概略図である。この携帯情報端末はデータ通信用携帯端末であり、直方体形状の筐体１を有し、この筐体１の主面１ａには、電話番号、文字などの入力、データ通信の開始、および通話などの通信機能の操作を行う通信機能操作部３と、液晶ディスプレイ２が設けられている。この通信機能操作部３に含まれるデータ通信開始キー３ａは、その内側から透過して画像認識を行い指紋を読みとれるように透明な樹脂で構成されており、指紋を読み取るために十分な大きさを持つ。データ通信開始キー３ａの内側には、そのキーの表面に接触した指の指紋を画像認識により読み取り、指紋データを生成する指紋読み取り装置が設けられている。データ通信開始キー３ａは、その押下によって、指紋読み取り装置を動作させるとともに、生成された指紋データに基づいてデータ通信の開始を指示する機能を持つ。また液晶ディスプレイ２は、通信機能操作部３によって入力される相手局電話番号表示、発信または着信メール表示などを行うとともに、後で説明する認証符号およびその有効期限を表示する表示手段である。

【００２６】図２は、実施の形態１の携帯情報端末の内部回路を示すブロック図である。通信機能操作部３の一つのキーであるデータ通信開始キー３ａは、そのキー操作に応じて指紋を読み取る手段である指紋読み取り装置４１と接続しており、データ通信開始キー３ａを押下することにより、指紋読み取り装置４１が動作し、使用者（ユーザ）の指紋を読み取る。指紋読み取り装置４１にて読み取られた指紋データは、制御部３６に送られる。制御部３６は、ＣＰＵ３７、あらかじめ登録された端末識別符号（端末ＩＤ）と使用者の指紋データを記憶している第１の記憶部３８、後で説明する認証符号（認証ＩＤ）とその有効期限を記憶する第２の記憶部３９、および照合手段４０から構成されており、第１、第２の記憶部３８、３９、および照合手段４０はＣＰＵ３７に接続されている。照合手段４０において制御部３６に送られた指紋データと第１の記憶部に記憶された指紋データの照合が行われる。ＣＰＵ３７は、この照合手段４０で一致が確認されると、本人認証を行うためのデータ通信を開始する制御を行う。

【００２７】本人認証を行うためのデータ通信が開始されると、指紋データは第１の記憶部３８から読み出された端末識別符号とともに暗号化手段３４において公開鍵暗号方式を用いて暗号化され、送信部３２によりアンテナ３１を介し送信される。ここで送信される指紋データは、一致が確認されているので、データ通信開始キー３ａが押下されたときに指紋読み取り装置４１によって読み取られたものでも、第１の記憶部３８にあらかじめ記憶されたものでもどちらでもよい。

【００２８】受信部３３は、後で説明するデータ処理装置で発行された認証符号とその有効期限をアンテナ３１より受信する。この認証符号および有効期限は公開鍵暗号方式を用いて暗号化されており、認証符号、有効期限ともに復号化手段３５によって復号化され、第２の記憶部３９に記憶されると同時に、液晶ディスプレイ２に表示される。また、この認証符号とその有効期限は、適宜、液晶ディスプレイ２に表示することが可能である。これにより、ユーザは認証符号の有効期限を必要に応じて確認することができ、有効期限の切れた認証符号を誤って使用することを防止する効果が得られる。

【００２９】また、この認証符号は、ユーザによって無効にすることが可能である。ＣＰＵ３７は、記憶部３８より端末識別符号を、記憶部３９より認証符号を読み出し、これらを暗号化手段３４において公開鍵暗号方式を用いて暗号化し、送信部３２により送信する制御を行う。後で説明するデータ処理装置は、端末識別符号と認証符号をあわせて受信すると、この認証符号を有効期限内であっても無効にする。これにより、携帯情報端末の盗難などにより、本人以外が認証符号を不正使用することを防止する効果が得られる。また、ユーザが認証符号を無効にすることを忘れる、あるいは回線トラブルなどで上記手続きによる無効ができなかった場合でも、あらかじめ適切な値に設定された有効期限により、本人以外が認証符号を不正使用することを防止できる。

【００３０】図３は実施の形態１におけるサービスシステムの構成図である。図に示すようにこのサービスシステムは、上記で説明した構成の携帯情報端末１２、データ処理装置４、およびサービス端末９を含んで構成されおり、それぞれはインターネット網８に接続可能である。データ処理装置４は、公的機関などに設けられるもので、あらかじめ使用者として登録された携帯情報端末

のユーザの指紋データと、その携帯情報端末を識別する端末識別符号とを対応させた指紋データ－端末識別符号情報（指紋ＤＢ）７を記憶した記憶部６、およびこれに接続されたコンピュータ５を備えており、コンピュータ５は、携帯情報端末１２から送信された端末識別符号に基づいて記憶部６より対応する指紋データを読み出し、この指紋データと携帯情報端末１２から送信された指紋データとを照合する照合機能を持つ。サービス端末９は、たとえばユーザに対しデータを提供するデータ提供業者、または商品を提供する商品販売業者などに設置されているものであって、ユーザから送信されたサービス依頼内容、認証符号などを一時的に記憶する記憶部１１、およびこれに接続されデータの入出力制御を行うコンピュータ１０を備えている。

【００３１】図４は、データ処理装置４に記憶された指紋データ－端末識別符号情報７のデータフォーマットを示している。端末識別符号１３および指紋データ１４はあらかじめ対応して登録されており、携帯情報端末１２から送信された指紋データと端末識別符号を照合の結果、本人認証がなされると、有効期限１６が設定された認証符号１５が発行され、同時に認証符号１５およびその有効期限１６が指紋データ－端末識別符号情報７に書き込まれる。

【００３２】次にこの実施の形態１の携帯情報端末およびこれを用いたサービスシステムの動作について、図５に示すフローチャートを用いて説明する。まず、携帯情報端末１２において、ユーザがデータ通信開始キー３ａを押下することにより、指紋読み取り装置４１が動作し指紋データの採取が行われる（ステップＳ５１）。採取された指紋データは、制御部３６に送られ、照合手段４０において、ＣＰＵ３７が第１の記憶部３８から読み出した指紋データと照合される（ステップＳ５２）。

【００３３】ステップＳ５３において、一致が確認されユーザがこの携帯情報端末１２の使用者であることが認証（本人認証）されると、データ通信が開始される。本人認証がされない場合は、本人認証に失敗したことが液晶ディスプレイ２に表示される（ステップＳ５４）。データ通信が開始されると、ＣＰＵ３７によって第１の記憶部３８から読み出された端末識別符号は指紋データとともに暗号化手段３４で公開鍵暗号方式を用いて暗号化され、送信部３２によりデータ処理装置４へ送信される（ステップＳ５５）。

【００３４】本人認証がされその結果に基づいてデータ通信が開始されるので、この携帯情報端末１２の登録された使用者以外がデータ処理装置４に対し端末識別符号および指紋データを送信することを防止できる。さらに、データ処理装置４が登録された使用者以外のデータを処理することを防止でき、不要な通信および処理を削減する効果が得られる。

【００３５】携帯情報端末１２が送信した端末識別符号と指紋データを受信したデータ処理装置４は、それらの復号化を行い、コンピュータ５が受信した指紋データと端末識別符号を記憶部６に記憶された指紋データ－端末識別符号情報７に照合する（ステップＳ５６）。ステップＳ５７において、コンピュータ５が一致を確認し、送信したユーザが携帯情報端末１２の登録された使用者であることを認証（本人認証）すると、有効期限が設定された認証符号が発行され、公開鍵暗号方式で暗号化されて携帯情報端末１２へ送信される。同時に認証符号およびその有効期限は、指紋データ－端末識別符号情報７に書き込まれ、コンピュータ５はタイマを張って、有効期限の管理を行う（ステップＳ５８）。

【００３６】ステップＳ５６において、本人認証がされない場合、データ処理装置４は、携帯情報端末１２へ本人認証が失敗したことを通知する（ステップＳ５９）。通知を受信した携帯情報端末１２は、本人認証が失敗したことを液晶ディスプレイ２に表示する（ステップＳ５４）。

【００３７】携帯情報端末１２は、データ処理装置４が発行し送信した認証符号を受信部３３で受信し復号化手段３５で復号化を行い、第２の記憶部に認証符号とその有効期限をあわせて記憶する（ステップＳ６０）。なお、記憶された認証符号とその有効期限は、液晶ディスプレイ２に表示が可能であり、ステップＳ６０において記憶部に記憶されるのと同時に表示されるとともに、認証符号を使用時に再度表示することが可能である。

【００３８】携帯情報端末１２のユーザは、サービス提供を依頼する場合、記憶した認証符号と依頼するサービス内容を暗号化手段３４にて公開鍵暗号方式を用いて暗号化し、送信部３２よりサービス端末９へ送信する（ステップＳ６１）。

【００３９】携帯情報端末１２が送信した認証符号とサービス内容を受信したサービス端末９は、受信した認証符号をデータ処理装置４へ送り、認証符号の確認を依頼する（ステップＳ６２）。データ処理装置４は、受信した認証符号に対応する指紋データ－端末識別符号情報７に書き込まれた有効期限を確認し（ステップＳ６３）、有効期限内であれば認証符号を確認した旨をサービス端末９へ返信する（ステップＳ６４）。受信した認証符号に対応する指紋データ－端末識別符号情報がない、または有効期限が切れている場合は、認証符号が確認できなかった旨をサービス端末９へ返信する（ステップＳ６５）。

【００４０】サービス端末９が認証符号を確認した旨の通知を得た場合は、携帯情報端末１２から依頼されたサービス内容が実施される（ステップＳ６６）。サービス端末９が認証符号を確認できなかった旨の通知を得た場合は、携帯情報端末１２に対し、依頼されたサービスを拒否する通知が行われる（ステップＳ６７）。

【００４１】以上のように、データ処理装置４におい

て、有効期限の定められた認証符号が発行され、携帯情報端末１２において、この認証符号をその有効期限とともに記憶するようにしたので、一度の本人認証手続きを行うことにより、有効期限内であれば何度でも認証符号を用いたサービス提供を依頼することが可能となる。

【００４２】また、携帯情報端末１２において、データ通信開始キー３ａの押下によって指紋読み取り装置４１が動作し、指紋が読み取られるようにしたので、使用者の使い勝手がよい。

【００４３】また、このサービスシステムにおいて通信される端末識別符号、指紋データ、認証符号およびサービス内容について、暗号化を行うようにしたので、セキュリティの高い本人認証手続きが可能となる。

【００４４】さらに、暗号化には公開鍵暗号方式を用いたので、データ処理装置４をインターネット上に設けることができる。

【００４５】なお、このサービスシステムにおいて通信される端末識別符号、指紋データ、認証符号およびサービス内容について、圧縮コード化を行っても良い。この場合、通信データ量を削減できるという効果が得られる。また、携帯情報端末は、通信機能を持つパソコンなどであっても良く、その場合も同様の効果が得られる。

【００４６】実施の形態２．図６はこの発明の実施の形態２である携帯情報端末の外観概略図である。図において、図１と同じ番号が付されたものは同じものを示すため説明を省略する。この携帯情報端末は、音声通話ができる電話機能を持つ携帯電話であり、通話相手の音声を出力するスピーカ１７とユーザの音声を入力するマイクロホン１８を備えている。３ｂは通信機能操作部３に含まれる通話開始キーであり、その内側から透過して画像認識を行い指紋を読みとれるように透明な樹脂で構成されており、指紋を読み取るために十分な大きさを持つ。通話開始キー３ｂの内側には、そのキーの表面に接触した指の指紋を画像認識により読み取り、指紋データを生成する指紋読み取り装置が設けられている。通話開始キー３ｂは、その押下によって、指紋読み取り装置を動作させるとともに、生成された指紋データに基づいて通話接続の開始を指示する機能を持つ。

【００４７】図７は、実施の形態２の携帯情報端末の内部回路を示すブロック図である。図において、図２と同じ番号が付されたものは同じものを示すため説明を省略する。３ｂは、通信機能操作部３の一つのキーであり、押下することにより、指紋読み取り装置４１が動作し、ユーザの指紋を読み取る。実施の形態１と同様にして読み取られた指紋データの一致が確認されると、本人認証を行うための通話接続手順が開始される。

【００４８】本人認証を行うための通話接続手順が開始されると、指紋データは端末識別符号とともに暗号化手段３４において後で説明する交換機とあらかじめ定められた暗号方式を用いて暗号化される。また、受信した認証符号は上記の暗号方式を用いて暗号化されており、復号化手段３５によって復号化される。

【００４９】また、レシーバ１７、マイクロホン１８は、制御部３６に含まれＣＰＵ３７に接続されたD／A変換器４２、A／D変換器４３にそれぞれ接続され、通話時に音声信号の入出力を行う。

【００５０】図８は実施の形態２におけるサービスシステムの構成図である。図に示すようにこのサービスシステムは、上記で説明した構成の携帯情報端末１２、実施の形態１で説明したデータ処理装置４に加えて、基地局などに設けられたものであって携帯情報端末１２とデータ処理装置４の通信の中継を行う交換機１９、および音声通話用電話であるサービス端末２３を含んで構成されおり、データ処理装置４と交換機１９はインターネット網８に接続されている。交換機１９は、携帯情報端末１２およびデータ処理装置４から受信する信号を所定の暗号方式で復号化する復号化手段２１と、携帯情報端末１２およびデータ処理装置４へ送信する信号を所定の暗号方式で暗号化する暗号化手段２０と、これらに接続され、認証結果に基づき認証符号をあらかじめ定められた対応する音声信号に変換する音声変換器２２とを備えている。サービス端末２３は、たとえばユーザに対し商品を提供する商品販売業者などに設置されているものであって、ユーザからのサービス依頼および本人認証結果を音声信号で受信する音声通話用電話である。

【００５１】次にこの実施の形態２の携帯情報端末およびこれを用いたサービスシステムの動作について、図９に示すフローチャートを用いて説明する。まず、携帯情報端末１２において、ユーザが本人認証を必要とするサービス依頼を行うためにサービス提供者の電話番号を入力し通話開始キー３ｂを押下し、これにより指紋読み取り装置４１が動作して指紋データの採取が行われる（ステップＳ７１）。採取された指紋データは、制御部３６に送られ、照合手段４０において、ＣＰＵ３７が第１の記憶部３８から読み出した指紋データと照合される（ステップＳ７２）。

【００５２】ステップＳ７３において、一致が確認されユーザがこの携帯情報端末１２の使用者であることが認証（本人認証）されると、通話接続手順が開始される。本人認証がされない場合は、本人認証に失敗したことが液晶ディスプレイ２に表示される（ステップＳ７４）。通話接続手順が開始されると、ＣＰＵ３７によって第１の記憶部３８から読み出された端末識別符号は指紋データとともに暗号化手段３４において、交換機１９との間であらかじめ定められた暗号方式で暗号化され、送信部３２により交換機１９へ送信される（ステップＳ７５）。

【００５３】交換機１９は、受信した指紋データと端末識別符号を復号化手段２１で一旦復号化し、さらに暗号化手段２０で公開鍵暗号方式を用いて暗号化して、イン

ターネット上のデータ処理装置４へ送信する（ステップＳ７６）。データ処理装置４は、受信した指紋データと端末識別符号の復号化を行い、コンピュータ５がそれらを記憶部６に記憶された指紋データー端末識別符号情報７に照合する（ステップＳ７７）。ステップＳ７８において、コンピュータ５が一致を確認し、送信したユーザを本人認証すると、有効期限が設定された認証符号が発行され、公開鍵暗号方式で暗号化されて交換機１９へ送信される。同時に認証符号およびその有効期限は、指紋データー端末識別符号情報７に書き込まれ、コンピュータ５はタイマを張って、有効期限の管理を行う（ステップＳ７９）。

【００５４】ステップＳ７８において、本人認証がされない場合、データ処理装置４は、交換機１９を経由して携帯情報端末１２へ本人認証が失敗したことを通知する（ステップＳ８０）。通知を受信した携帯情報端末１２は、本人認証が失敗したことを液晶ディスプレイ２に表示する（ステップＳ７４）。

【００５５】認証符号を受信した交換機１９は、それを復号化手段２１で一旦復号化し、さらに暗号化手段２０で携帯情報端末１２との間であらかじめ定められた暗号方式を用いて暗号化して携帯情報端末１２へ送信するとともに、ユーザがサービス依頼を行う相手であるサービス端末２３へ通話を接続する処理を行い、サービス端末２３へサービス依頼主が本人認証された旨を音声信号で通知する（ステップＳ８１）。

【００５６】このとき通知する音声信号は、音声変換器２２で生成されたものであって、たとえば「サービス依頼主は認証符号××××号によって本人認証された端末識別符号××××××の携帯情報端末の使用者です」などとする。サービス端末２３が本人認証された旨の通知を受け、通話によってサービスが依頼されると、サービス内容が実施される（ステップＳ９６）。

【００５７】交換機１９から認証符号を受信した携帯情報端末１２は、復号化を行い、第２の記憶部に認証符号とその有効期限をあわせて記憶する（ステップＳ８２）と同時に、液晶ディスプレイ２に表示する。

【００５８】有効期限内に別のサービス提供依頼に対し上記の説明で取得した認証符号を使用する場合は、携帯情報端末１２は認証符号を暗号化して交換機１９に送付する（ステップＳ９１）。交換機１９は受信した認証符号をデータ処理装置４に送り、認証符号の確認を行う（ステップＳ９２）。ステップＳ９３において、認証符号が有効期限内であることを確認されると、交換機１９は、ユーザがサービス依頼を行う相手であるサービス端末２３と携帯情報端末１２の通話を接続する処理を行い、サービス端末２３へサービス依頼主が本人認証された旨を音声信号で通知する（ステップＳ９４）。サービス端末２３が本人認証された旨の通知を受け、通話によってサービスが依頼されると、サービス内容が実施される（ステップＳ９６）。

【００５９】ステップＳ９３において、認証符号が有効期限内であることが確認されなかった場合、交換機１９は、認証されなかった旨を携帯情報端末１２へ通知し（ステップＳ９５）、通知を受信した携帯情報端末１２は、本人認証が失敗したことを液晶ディスプレイ２に表示する（ステップＳ７４）。

【００６０】以上のように、データ処理装置４において、有効期限の定められた認証符号が発行され、携帯情報端末１２において、この認証符号をその有効期限とともに記憶するようにしたので、一度の本人認証手続きを行うことにより、有効期限内であれば何度でも認証符号を用いたサービス提供を依頼することが可能となる。

【００６１】また、携帯情報端末１２において、通話開始キー３ｂの押下によって指紋読み取り装置４１が動作し、指紋が読み取られるようにしたので、使用者の使い勝手がよい。

【００６２】また、このサービスシステムにおいて通信される端末識別符号、指紋データ、認証符号およびサービス内容について、暗号化を行うようにしたので、セキュリティの高い本人認証手続きが可能となる。

【００６３】さらに、このサービスシステムに交換機を含み、交換機が、本人認証の確認された旨を音声信号にてサービス端末へ通知するようにしたので、サービス端末はデータ通信機能のない電話機でもよく、使い勝手が良い。

【００６４】

【発明の効果】以上のようにこの発明によれば、データ処理装置において、有効期限の定められた認証符号を発行し、携帯情報端末において、この認証符号をその有効期限とともに記憶するようにしたので、一度の本人認証を行うことにより、複数のサービス提供を受けることができる。

【００６５】また、この発明によれば、指紋データおよび認証符号を暗号化して送信するようにしたので、セキュリティに優れた携帯情報端末を提供できる。

【００６６】また、この発明によれば、指紋データおよび認証符号の暗号化を公開鍵暗号方式を用いて行うようにしたので、データ処理装置をインターネット上に設けることができる。

【００６７】また、この発明によれば、指紋データおよび認証符号を圧縮コード化して送信するようにしたので、送受信するデータ量の少ない携帯情報端末を提供できる。

【００６８】また、この発明によれば、携帯情報端末において、取得した認証符号とその有効期限を表示するようにしたので、有効期限の確認が容易にでき、使い勝手がよい。

【００６９】また、この発明によれば、携帯情報端末において、記憶部に記憶した認証番号を無効にするように

したので、本人以外が不正にサービスの提供を受けることを防止できる。

【００７０】また、この発明によれば、携帯情報端末のデータ通信開始キーまたは通話開始キーに指紋読み取り手段を設けたので、通信の開始動作によって指紋データの採取が行われ、使い勝手がよい。

【００７１】また、この発明によれば、携帯情報端末において指紋データの照合を行い、本人認証後に端末識別符号および指紋データを送信するようにしたので、利用者の制限ができる。

【００７２】また、この発明によれば、サービスシステムに交換機を含み、交換機が、認証符号を対応する音声信号に変換してサービス端末へ通知するようにしたので、サービス端末はデータ通信機能のない電話機でもよく、使い勝手が良いサービスシステムを提供できる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１における携帯情報端末の外観概略図である。

【図２】　本発明の実施の形態１における携帯情報端末の内部回路を示すブロック図である。

【図３】　本発明の実施の形態１におけるサービスシステムの構成図である。

【図４】　本発明の実施の形態１における指紋データ－端末識別符号情報のデータフォーマット図である。

【図５】　本発明の実施の形態１における携帯情報端末およびサービスシステムの動作を示すフローチャートである。

【図６】　本発明の実施の形態２における携帯情報端末の外観概略図である。

【図７】　本発明の実施の形態２における携帯情報端末の内部回路を示すブロック図である。



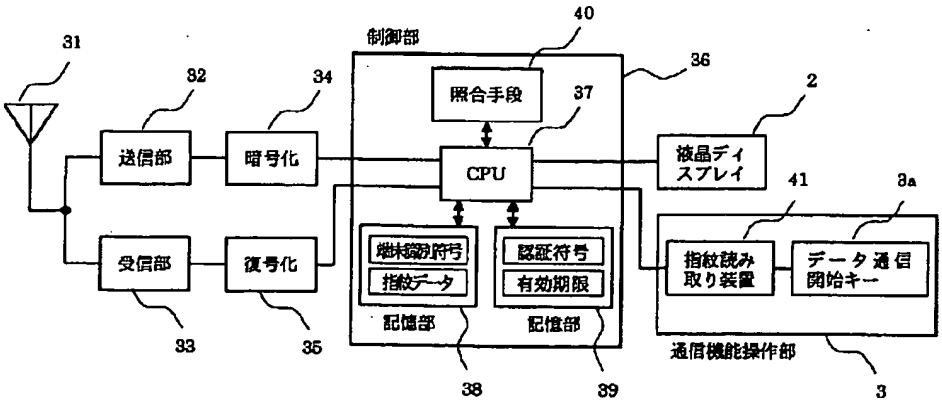
【図８】　本発明の実施の形態２におけるサービスシステムの構成図である。

【図９】　本発明の実施の形態２における携帯情報端末およびサービスシステムの動作を示すフローチャートである。

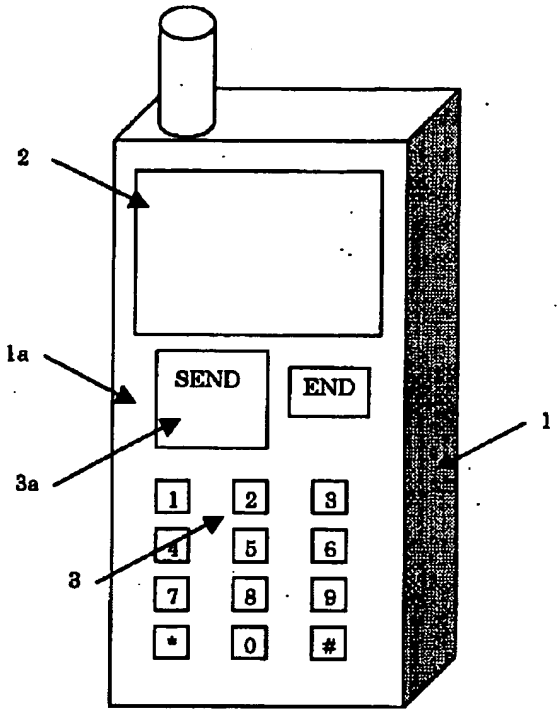
【符号の説明】

２　液晶ディスプレイ（表示手段）
３　通信機能操作部
３ａ　データ通信開始キー
３ｂ　通話開始キー
４　データ処理装置
５　コンピュータ（照合手段）
６　記憶部
７　指紋データ?端末識別符号情報
９　サービス端末
１２　携帯情報端末
１３　端末識別符号
１４　指紋データ
１５　認証符号
１６　認証符号有効期限
１９　交換機
２３　サービス端末
３２　送信部
３３　受信部
３４　暗号化手段
３５　復号化手段
３７　ＣＰＵ
３８　記憶部
３９　記憶部
４０　照合手段
４１　指紋読み取り装置（指紋読み取り手段）

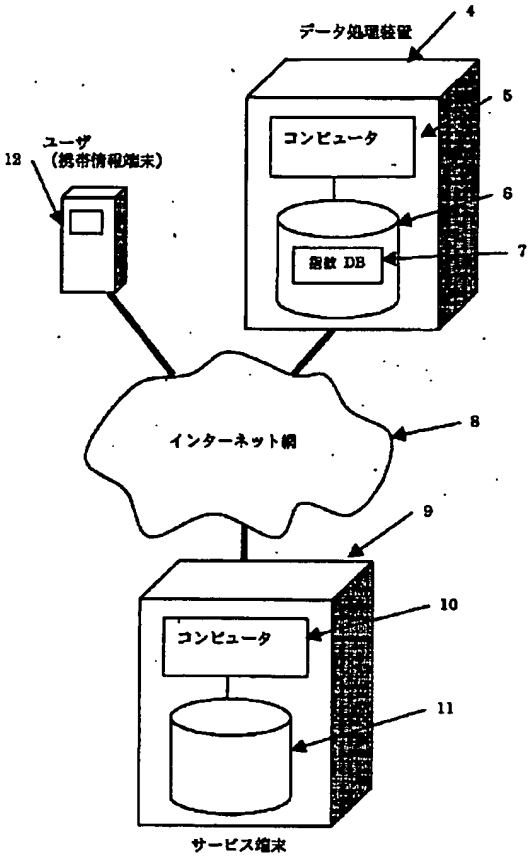
【図２】



【図1】



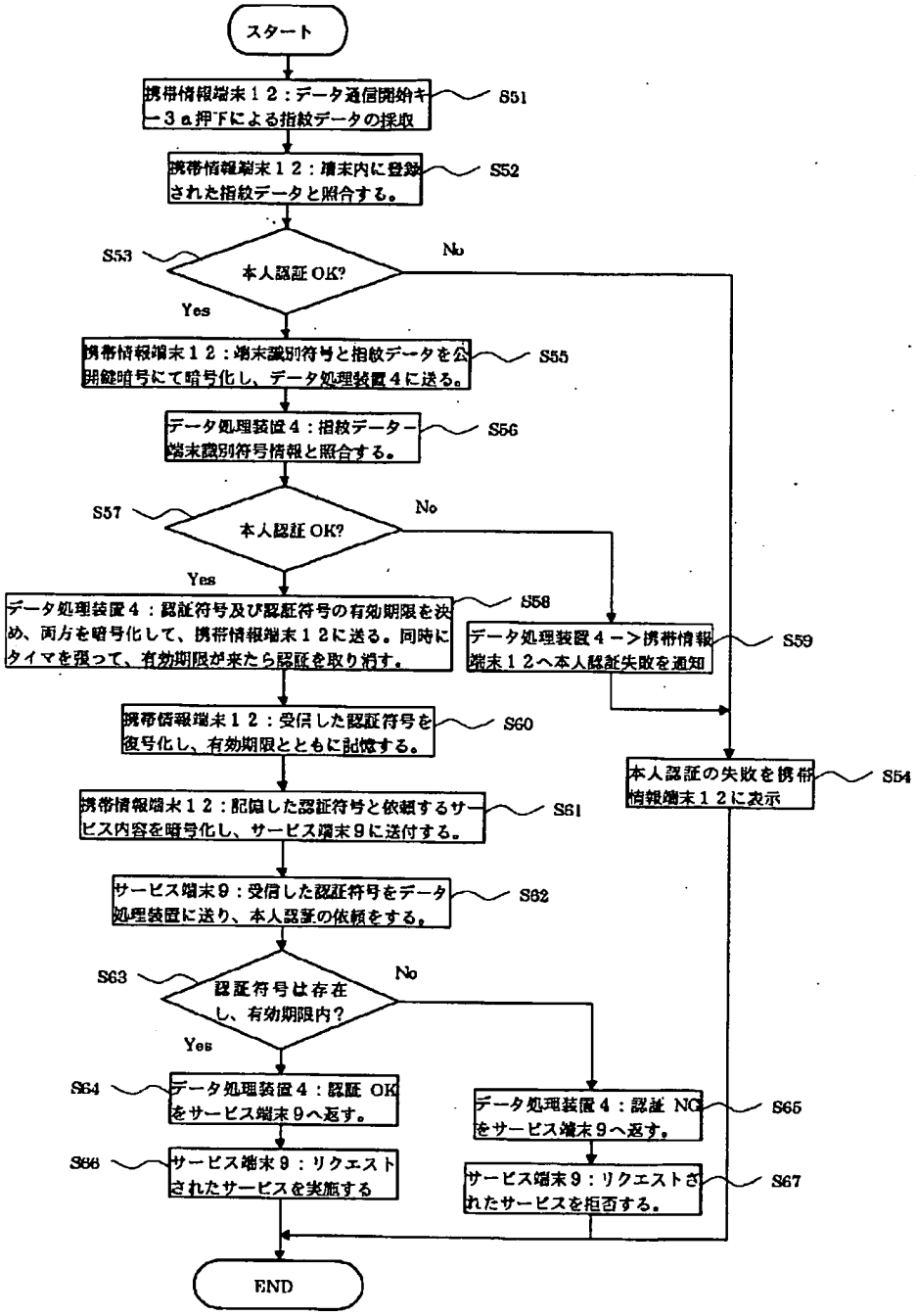

【図3】



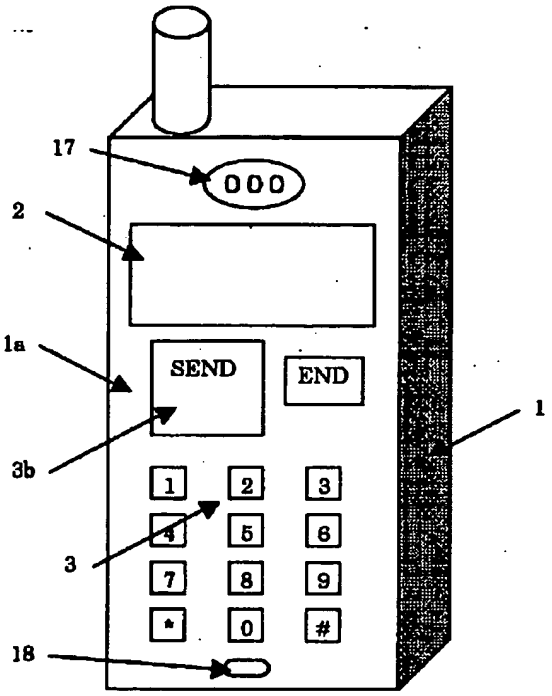

【図4】

| 端末識別符号 | 指紋データ | 認証符号 | 認証符号有効期限 |
|---|---|---|---|
| 1234567890 | User 指紋 Data | 00000001 | 00/02/25 15:15:30 |
| 1234567891 | User 指紋 Data | 0 | — |
| : | : | : | : |

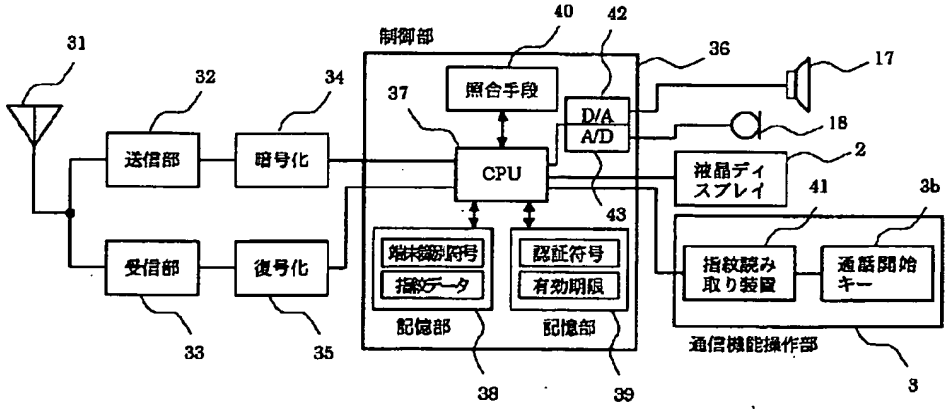
【図5】


スタート
携帯情報端末１２：データ通信開始キー３ａ押下による指紋データの採取
S51
携帯情報端末１２：端末内に登録された指紋データと照合する。
S52
S53
本人認証OK?
No
Yes
携帯情報端末１２：端末識別符号と指紋データを公開鍵暗号にて暗号化し、データ処理装置４に送る。
S55
データ処理装置４：指紋データ－端末識別符号情報と照合する。
S56
S57
本人認証OK?
No
Yes
データ処理装置４：認証符号及び認証符号の有効期限を決め、両方を暗号化して、携帯情報端末１２に送る。同時にタイマを張って、有効期限が来たら認証を取り消す。
S58
データ処理装置４－＞携帯情報端末１２へ本人認証失敗を通知
S59
携帯情報端末１２：受信した認証符号を復号化し、有効期限とともに記憶する。
S60
本人認証の失敗を携帯情報端末１２に表示
S54
携帯情報端末１２：記憶した認証符号と依頼するサービス内容を暗号化し、サービス端末９に送付する。
S61
サービス端末９：受信した認証符号をデータ処理装置に送り、本人認証の依頼をする。
S62
S63
認証符号は存在し、有効期限内?
No
Yes
S64
データ処理装置４：認証 OK をサービス端末９へ返す。
データ処理装置４：認証 NG をサービス端末９へ返す。
S65
S66
サービス端末９：リクエストされたサービスを実施する
サービス端末９：リクエストされたサービスを拒否する。
S67
END

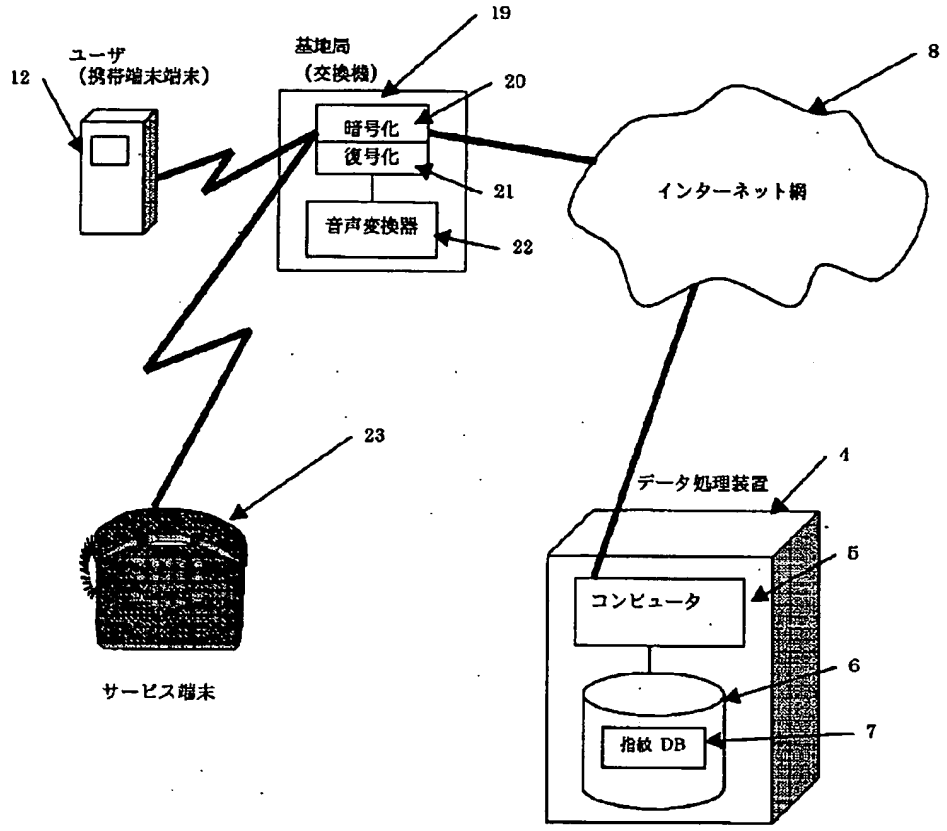
【図6】


17
000
2
1a
SEND
END
1
3b
1
2
3
4
5
6
3
7
8
9
*
0
#
18

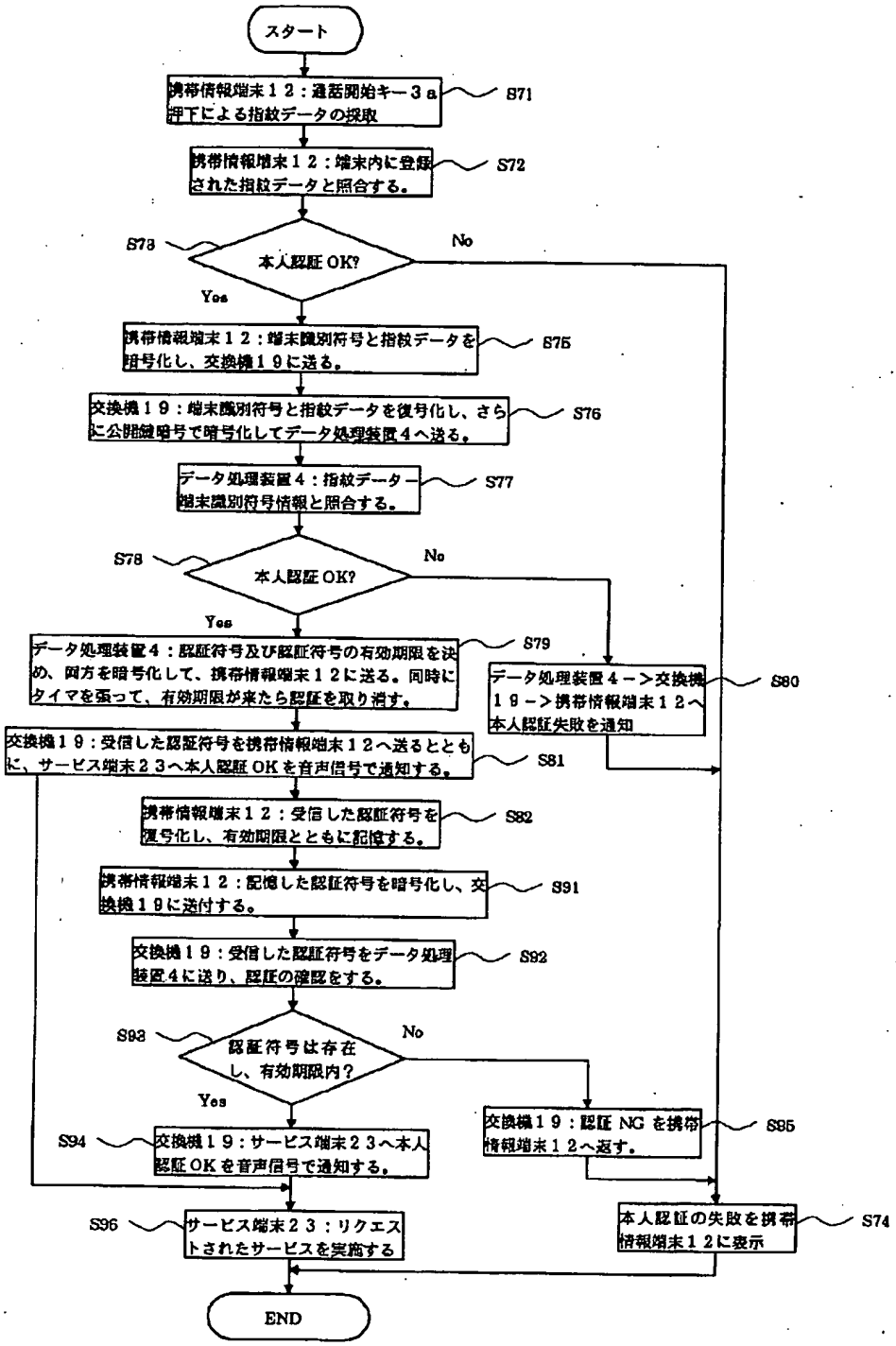
【図7】


31
32
34
制御部
40
42
36
17
照合手段
37
D/A
A/D
18
2
送信部
暗号化
CPU
液晶ディスプレイ
41
3b
43
端末識別符号
指紋データ
認証符号
有効期限
指紋読み取り装置
通話開始キー
受信部
復号化
記憶部
記憶部
通信機能操作部
33
35
38
39
3

【図8】


ユーザ
（携帯端末端末）
12
基地局
（交換機）
19
20
暗号化
復号化
21
音声変換器
22
8
インターネット網
23
サービス端末
4
データ処理装置
5
コンピュータ
6
指紋 DB
7

【図9】


スタート
携帯情報端末１２：通話開始キー３ａ押下による指紋データの採取
S71
携帯情報端末１２：端末内に登録された指紋データと照合する。
S72
S73
本人認証 OK?
No
Yes
携帯情報端末１２：端末識別符号と指紋データを暗号化し、交換機１９に送る。
S75
交換機１９：端末識別符号と指紋データを復号化し、さらに公開鍵暗号で暗号化してデータ処理装置４へ送る。
S76
データ処理装置４：指紋データ－端末識別符号情報と照合する。
S77
S78
本人認証 OK?
No
Yes
データ処理装置４：認証符号及び認証符号の有効期限を決め、両方を暗号化して、携帯情報端末１２に送る。同時にタイマを張って、有効期限が来たら認証を取り消す。
S79
データ処理装置４－＞交換機１９－＞携帯情報端末１２へ本人認証失敗を通知
S80
交換機１９：受信した認証符号を携帯情報端末１２へ送るとともに、サービス端末２３へ本人認証 OK を音声信号で通知する。
S81
携帯情報端末１２：受信した認証符号を復号化し、有効期限とともに記憶する。
S82
携帯情報端末１２：記憶した認証符号を暗号化し、交換機１９に送付する。
S91
交換機１９：受信した認証符号をデータ処理装置４に送り、認証の確認をする。
S92
S93
認証符号は存在し、有効期限内？
No
Yes
交換機１９：認証 NG を携帯情報端末１２へ返す。
S95
S94
交換機１９：サービス端末２３へ本人認証 OK を音声信号で通知する。
本人認証の失敗を携帯情報端末１２に表示
S74
S96
サービス端末２３：リクエストされたサービスを実施する
END

フロントページの続き

| (51)Int.Cl.[7] | 識別記号 | FI | | テーマコード(参考) |
|---|---|---|---|---|
| H04M 3/42 | | H04B 7/26 | | 109R 5K101 |
| 11/00 | 302 | H04L 9/00 | | 673D 9A001 |
| | | | | 673A |

Fターム(参考) 5J104 AA07 KA01 KA17 PA02 PA10
5K024 AA62 AA76 CC11 DD01 DD02
DD04 FF05 GG01 GG05
5K027 AA11 BB09 HH23
5K051 CC01 JJ07 JJ13 JJ16 JJ17
5K067 AA33 BB00 BB04 BB21 EE02
EE16 GG01 GG11 HH05 HH22
HH23 HH24
5K101 LL12 NN06 PP04
9A001 EE03 EE04 EE05 JJ25 LL03